01 Réseaux

N° 139 / Mai 2004 / 4,60 €

LE PREMIER MAGAZINE DES TECHNOLOGIES DE L'INFORMATION

internet Professionnel

Extrait de 01 Réseaux 139

DOSSIER THÉMATIQUE

SÉCURITÉ

associer servi... équ...

"Le service d'audit de vunérabilité de Qualys recommandé par la rédaction de 01 Réseaux "

L'ÉVÉNEMENT

Sun et Microsoft

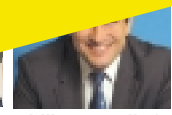

Deux milliards de dollards mettent fin à sept ans de guerre autour de Java.

TENDANCE

Le retour des ateliers de génie logiciel

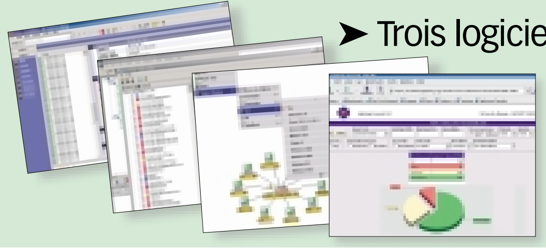
➤ Les ...


Philippe Germond, d'Alcatel


Philippe Carli, de Siemens France

BANC D'ESSAI COMPARATIF

4 solutions pour déceler les failles de sécurité



➤ Trois logiciels et un service d'audit en ligne qui détectent les vulnérabilités des serveurs et des réseaux testés par notre laboratoire.

MISE EN ŒUVRE

Les formulaires électroniques deviennent dynamiques

➤ XML et le concept de client riche modifient la donne des formulaires électroniques. Ils sortent de leur statisme et deviennent adaptables.



3 logiciels et un ser

Pour déceler les failles de sé

Trois logiciels sous licence et un service d'audit de vulnérabilités ont été testés sur une plate-forme hétérogène avec neuf systèmes d'exploitation serveurs et des équipements réseaux. La pertinence de l'identification des failles de sécurité et l'exhaustivité de l'inventaire placent en tête Qualys et son boîtier relié à un serveur en ligne.

Comment détecter et corriger les vulnérabilités et autres failles de sécurité rampantes qui mettent potentiellement en danger le réseau et les serveurs d'une entreprise ? Des outils spécialisés répondent à ce besoin en analysant les serveurs et les équipements de réseau qui leur sont soumis. Ils sont aussi censés fournir une vue exhaustive, sous forme d'inventaire, des versions de logiciels d'exploitation et des services (FTP et Telnet, par exemple) de l'infrastructure qu'ils examinent via une connexion locale en Ethernet. Notre laboratoire a sélectionné quatre solutions. Trois d'entre elles sont constituées de logiciels indépendants, commercialisés sous forme de licences : Retina Network Security Scanner, d'eEye Digital Security ; Internet Scanner, d'Internet Security Systems (ISS) ; et l'ensemble Nessus et Lightning Console, de Tenable Network Security. Le quatrième participant à ce banc d'essai est un service en ligne, QualysGuard Intranet Scanner, de Qualys. Il est fourni avec un boîtier dédié à la détection des vulnérabilités, connecté en SSL via internet à un serveur distant. Les rapports sont mis en ligne sur un serveur de Qualys à l'issue des tests. Même si l'éditeur offre toutes les garanties de chiffrement des données, il faut néanmoins confier à un prestataire extérieur les données confidentielles (tel un rapport sur les vulnérabilités d'un réseau d'entreprise).

Des audits programmables pour tous les produits

À l'aune des cinq critères d'évaluation retenus, la solution QualysGuard Intranet Scanner domine ses concurrents logiciels autant par sa simplicité d'installation et d'administration que par la richesse fonctionnelle proposée et la quantité d'informations remontées. Nous émettons toutefois une réserve, qui tient à la nature même d'un tel service externalisé. Sur le plan méthodologique, nous avons supposé que le service fourni était un service standard. Les deux critères jugés les plus importants ont concerné, d'une part, la pertinence de l'audit des vulnérabilités détectées par les scanners, et, d'autre part, le degré d'exhaustivité de l'inventaire des systèmes installés, de leurs systèmes d'exploitation et des services. Trois autres critères viennent en complément : rapports et alertes ; facilité d'emploi et sécurité ; et gestion des vulnérabilités.

Pour évaluer la pertinence de l'audit des vulnérabilités, nous avons regardé comment se comportaient les quatre outils face aux failles de sécurité (vulnérabilités RPC, Sendmail, SNMP et FTP ou comptes insuffisamment verrouillés, par exemple) de la plate-forme de test comprenant serveurs, systèmes d'exploitation et équipements réseaux. QualysGuard obtient les meilleurs résultats dans la détection des vulnérabilités (lire le tableau p. 119). Il se distingue tout particulièrement sur les failles d'administration SNMP des équipements réseaux, qu'il s'agisse du commutateur 3Com ou du routeur Cisco Systems. Il obtient également les meilleurs résultats sur les failles RPC et sur les comptes insuffisamment verrouillés. Cette solution est toutefois non intrusive dans sa version actuelle, au sens où il n'était pas possible d'effectuer des attaques pour tester la vulnérabilité de l'infrastructure.

Le scanner d'eEye Digital Security se distingue seulement par ses résultats de remontée de vulnérabilités sur le serveur Sun-Solaris. Celui d'ISS trouve bien les

Si vous êtes pressé...

▶ **Trois logiciels d'analyse de vulnérabilités** ont été passés au crible, ainsi que la solution de Qualys, vendue comme un service, couplant un boîtier à un serveur internet. Les quatre produits ont été testés dans un environnement composé de serveurs hétérogènes, avec neuf systèmes d'exploitation différents, et divers équipements réseaux.

▶ **Le service de Qualys domine** tant par sa simplicité d'administration que par la quantité et la pertinence des informations remontées.

▶ **eEye Digital Security et ISS** proposent chacun un outil sous Windows. Les interfaces utilisateurs et les rapports d'audits, avec Retina, sont plutôt soignés.

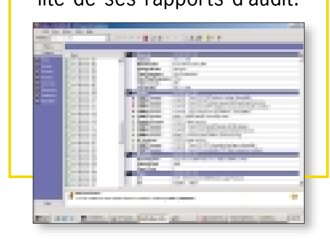
▶ **Le logiciel de Tenable, sous Linux,** s'est révélé le moins évident à installer. Il offre cependant une bonne gestion des correctifs, palliant les vulnérabilités, avec leur suivi.



vice d'audit en ligne
curité des serveurs et réseaux

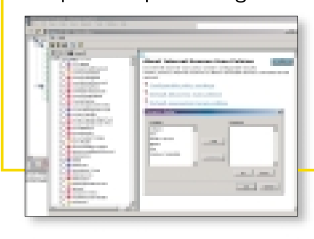
EEYE DIGITAL SECURITY
Retina Network Security Scanner

Ce logiciel sous Windows a moyennement détecté les vulnérabilités de la plate-forme de test. Il se distingue par la qualité de ses rapports d'audit.



INTERNET SECURITY SYSTEMS
Internet Scanner

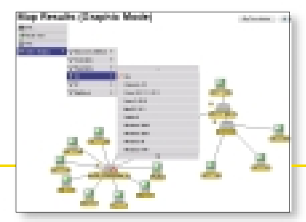
Ce scanner sous Windows a surtout détecté les vulnérabilités liées à… Windows, et non les autres. Il se différencie par sa simplicité de paramétrage.



Recommandé 01 Réseaux LABO TESTS
pour les petits et moyens sites

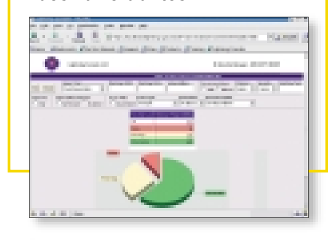
QUALYS
QualysGuard Intranet Scanner

Basé sur un boîtier relié par internet à des serveurs distants, ce service en ligne se distingue par la pertinence de l'identification des systèmes et de leurs vulnérabilités.



TENABLE
Nessus et Lightning Console

Seul logiciel fonctionnant sur Linux, ce scanner s'est montré meilleur dans l'identification des systèmes que dans la détection des vulnérabilités.



vulnérabilités Windows, mais plus difficilement celles des équipements de commutation et celles qui interviennent sous Solaris. Nessus a, lui aussi, eu du mal à détecter les failles des équipements réseaux. Il est à noter qu'aucun outil n'a relevé de fausse vulnérabilité. Les réglages proposés sur tous les produits permettent une programmation temporelle pour planifier les audits. Il est possible de paramétrer une heure de fin de *scan*. Excepté Qualys, les constructeurs proposent un mode – optionnel – de tests agressifs (faisant réellement les attaques) pour s'assurer de la véracité des vulnérabilités trouvées.

Une bonne détection des systèmes d'exploitation

L'inventaire du réseau a été évalué sur la base d'une plate-forme de tests hétérogène en termes de serveurs, de systèmes d'exploitation (Linux, Solaris, Mac OS X, et Windows et ses différentes versions) et d'équipements réseaux (2 routeurs Cisco et un commutateur Ethernet 3Com). Chez les quatre fournisseurs, le scanner découvre toutes les machines installées sur notre plate-forme. Aucun, en revanche, n'a identifié la substitution d'une station par une autre lorsque l'adresse IP était conservée. Seul Nessus, lors d'un nouveau *scan*, a détecté la nouvelle machine, mais il n'indique pas qu'il s'agit d'un changement de configuration. De façon générale, toutes les solutions détectent assez bien les treize systèmes d'exploitation de la plate-forme (y compris ceux qui sont embarqués dans les équipements réseaux). QualysGuard Intranet Scanner arrive en tête. C'est Nessus qui a le moins bon résultat (9 systèmes d'exploitation sur 13 ont été découverts). Il distingue mal Windows 2000 de Windows XP. Il n'a pas identifié non plus un XP sur lequel un pare-feu filtrait le protocole ICMP, ainsi que le second routeur. Quel que soit l'outil d'analyse, le Macintosh et le Solaris n'ont pas été décelés convenablement. Ainsi, Retina Network Security Scanner a identifié un HP-UX à la place de Mac OS X du G5 d'Apple, et QualysGuard Intranet Scanner a reconnu la version 8 de Solaris au lieu de la version 5.8. Les solutions ont, en général, bien découvert les services usuels des systèmes. Un petit bémol chez ISS, cependant, où les versions ne sont pas indiquées dans l'interface, mais dans le rapport. Notons que l'éditeur adapte ses audits selon le système d'exploitation et des ports, à condition de laisser activé le mode DCA *(Dynamic check assignment)*. Qualys permet, quant à lui, de cartographier le réseau.

> LE MACINTOSH ET LE SOLARIS N'ONT PAS ÉTÉ CONVENABLEMENT DÉCELÉS, QUEL QUE SOIT L'OUTIL D'ANALYSE.

Afin de corser les tests, notre laboratoire a dissimulé quatre services réseaux derrière des ports inhabituels (HTTP derrière le port 12345, FTP derrière le port 1433 dédié à MS-SQL, Telnet derrière le port 21, et FTP derrière le port 80). QualysGuard les a tous repérés. Nessus en reconnaît trois sur quatre. En revanche, Internet Scanner et Retina n'ont trouvé, respectivement, qu'un et deux services sur les quatre dissimulés. En matière de rapports générés par les logiciels, le laboratoire n'en a considéré que deux : le rap- ▸

▶ port exécutif, peu technique, censé présenter la tendance du réseau au directeur du système d'information, et le rapport technique fournissant à l'administrateur système le détail des vulnérabilités rencontrées. Retina et QualysGuard affichent les meilleurs rapports exécutifs grâce aux graphiques proposés (camemberts indiquant les niveaux de risques rencontrés, les vulnérabilités les plus fréquentes et les machines les plus stratégiques). Chez Retina, les rapports sont axés par machine auditée et par groupe de fonctionnalité (audit, machine, port, service et partage), ce qui facilite la tâche de l'administrateur non spécialisé en sécurité.

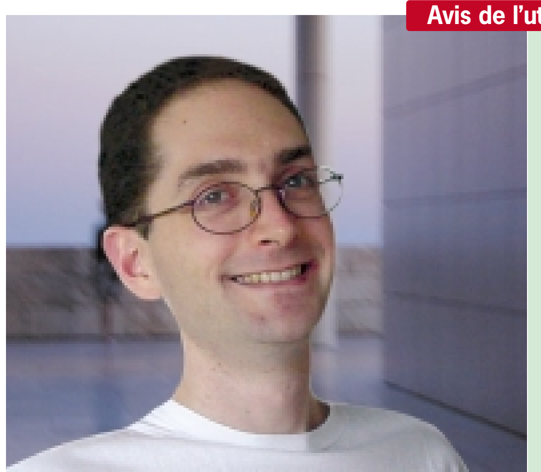
Des rapports d'activités envoyés directement à l'administrateur

Sur QualysGuard, on remarque aussi l'exhaustivité des informations remontées pour le rapport technique : description de la vulnérabilité, conséquence et solution détaillée. Chez ISS, en revanche, la présentation est bien faite, mais les rapports manquent de consistance. Chez Nessus, la présentation des rapports techniques est correcte, et les exposés des vulnérabilités et parades sont assez exhaustifs. Notons encore que Nessus et Retina permettent l'envoi d'alertes à l'administrateur système lorsqu'une machine vulnérable est détectée. Cette particularité apporte un plus, les analyseurs de vulnérabilités n'étant pas censés protéger en temps réel le réseau.
Concernant la facilité d'emploi, la solution de Qualys apparaît comme la meilleure en termes de déploiement et d'administration. La configuration initiale du boîtier consiste à entrer son identifiant à partir de l'écran LCD et l'adresse IP. Des rapports d'activités sont directement envoyés à l'administrateur. La solution de Tenable est perfectible sur ce point. Son installation et son utilisation requièrent des notions avancées en informatique (malgré une bonne documentation !). Par contre, l'exécution du premier *scan* est plutôt simple. Pour faire fonctionner le scanner d'eEye Digital Security, il faut installer SQL 2000, Windows 2000 SP3 et MSXML, puis tous les modules, avant de les interfacer. L'exécution du premier *scan*, par défaut, est assez simple. Il faut au préalable déterminer les plages d'adresses IP et les règles souhaitées. Le premier scan, par défaut, du produit d'ISS est aussi très simple. Il est possible de visualiser en temps réel les résultats du *scan*. En sécurité, Qualys propose le transfert sécurisé en SSL des données entre le boîtier et le serveur. Il en est de même pour l'envoi des rapports à l'administrateur, les mises à jour et le stockage des rapports. Nous avons aussi apprécié une gestion de comptes avec des droits limités. Chez Tenable, le stockage des résultats n'est pas sécurisé (mais on peut chiffrer la partition d'hébergement de la base), et l'envoi sécurisé des rapports est optionnel. Nous avons toutefois prisé le cryptage SSL entre la console et le scanner, une gestion de comptes avec des droits limités, et la mise à jour en ligne sécurisée. Chez eEye Digital Security, le scanner et la console sont sur la même machine. Il est donc inutile de sécuriser leurs échanges. Le seul reproche à lui faire est de ne pas avoir de compte d'administration. Chez ISS, les mises à jour en ligne sont sécurisées. Pour finir, la gestion des vulnérabilités a été examinée sur chacun des quatre outils. Tous (sauf Retina) s'avèrent com-

FAILLES ET SERVICES CACHÉS SONT DÉTECTÉS INÉGALEMENT

Informations sur les failles	Retina Network Security Scanner	Internet Scanner	QualysGuard Intranet Scanner	Nessus + Lightning Console
Identification de services réseaux dissimulés				
Telnet sur port 21	non	non	oui	oui
FTP sur port 80	non	non	oui	oui
Failles détectées				
W 98 SE : compte admin. sans mot de passe	oui	oui	non	non
W 2000 : compte admin. sans mot de passe	oui	oui	oui	oui
Cisco 1720 : login = cisco, mot de passe = cisco	non	non	oui	non
3Com : login admin. sans mot de passe	non	non	oui	non

Tous les scanners ont identifié des informations sur les vulnérabilités propres aux machines en réseau de la plate-forme de test. Les résultats obtenus ont été comparés avec la configuration de chaque machine. Aucun outil n'a relevé de fausses vulnérabilités.



Avis de l'utilisateur

« La détection de vulnérabilité apporte une certaine tranquillité d'esprit »

▶ **Laurent Muller,** directeur général et directeur informatique du groupe Alban Muller

Le groupe Alban Muller, qui fabrique des matières premières naturelles pour l'industrie cosmétique, a opté, depuis mars 2001, pour le service QualysGuard, de Qualys. La PME, qui dispose de trois sites, a choisi le service en mode externe, assuré, depuis un serveur Qualys, via une liaison IP permanente avec son site principal de Vincennes (94). Elle possède trois serveurs connectés en permanence à internet, tous situés à Vincennes. Le service est calibré pour quatre adresses IP. Quand on procède à des changements sur nos serveurs informatiques, nous lançons systématiquement un *scan* manuel. Cela nous assure une certaine tranquillité d'esprit. Sinon, la PME effectue un audit de vulnérabilité hebdomadaire, lancé en fin de semaine pour ne pas perturber l'activité informatique. Elle consulte le rapport de cette analyse sur le serveur de Qualys, via une liaison sécurisée SSL à 128 bits. Nous apprécions les préconisations de résolution des failles de sécurité incluses dans le service.

patibles avec les nomenclatures CVE, Bugtraq ID et Cert, qui recensent les principales vulnérabilités. Le classement des vulnérabilités est en revanche différent d'un éditeur à l'autre.

Des conseils pour pallier les vulnérabilités

Qualys et ISS proposent de bonnes fonctions (tris variés, détails CVE et vulnérabilités les plus actives), mais eEye Digital Security doit revoir sa copie : la catégorie *Miscenaleous* (divers) est très (trop) remplie ! Si toutes les solutions proposent des recommandations pour pallier les vulnérabilités, seuls Qualys et Tenable permettent à l'administrateur une gestion des interventions et un suivi des correctifs. Chez Tenable, il est possible d'éditer des rapports avec une vue cumulative des anciens *scans* ; chez Qualys, un délai de correction et une échéance sont mentionnés. Le scanner Retina ne dispose pas d'outil de suivi de correctifs, mais cette fonction est disponible avec la solution complémentaire EVA *(Enterprise vulnerability assessment)*. Enfin, Nessus et Qualys proposent le contrôle centralisé de plusieurs scanners de même marque. ■

FRÉDÉRIC BERGÉ

LEXIQUE

■ **Mode découverte :** mode permettant au scanner d'établir la liste des stations, serveurs et équipements à partir d'un sous-réseau IP.

■ **CVE** *(Common vulnerabilities and exposures) :* liste standardisée de noms de vulnérabilités et autres failles de sécurité (www.cve.mitre.org). Il s'agit d'un dictionnaire plus que d'une base. La version publiée au moment de nos tests était la 20030402.

LABO GROUPE TESTS méthodologie

Les quatre produits ont été évalués selon cinq critères.

■ PERTINENCE DE L'AUDIT

Nous avons repéré plusieurs vulnérabilités (failles de sécurité et mauvaises configurations), et avons regardé comment se comportaient les outils d'audit. Chacun des scanners a remonté des informations spécifiques aux systèmes d'exploitation, services et vulnérabilités propres aux machines de la plate-forme. Les résultats obtenus ont été comparés avec la configuration précise de chaque machine IP détectée et analysée par les logiciels.

■ INVENTAIRE ET DÉCOUVERTE

La gestion d'inventaire consiste en la découverte des nœuds du réseau et la détection-identification des systèmes d'exploitation et des services à la fois usuels et dissimulés. La détection d'une intrusion par substitution de poste a été testée. Afin de corser les tests, nous avons également dissimulé quatre services derrière des ports inhabituels (HTTP sur le port 12345, FTP sur le port 1433, Telnet sur le port 21 et FTP sur le port 80). La plate-forme était composée de serveurs sous systèmes d'exploitation Microsoft (98 SE, NT 4, 2000, 2000 Pro, XP, 2003), Linux Red Hat 9, Solaris 5.8 et Mac OS X (Apple G5). Ont été ajoutés un point d'accès radio 802.11b Cisco, deux routeurs Cisco (1720 et 1750) et un commutateur 3Com avec chacun un système d'exploitation différent.

■ RAPPORTS ET ALERTES

Deux types de rapports ont été considérés. Le rapport exécutif – visé par le responsable d'exploitation –, qui n'est pas forcément technique. Et le rapport technique, qui énumère les vulnérabilités rencontrées.

■ FACILITÉ D'EMPLOI ET SÉCURITÉ

La facilité de mise en place du produit a été jugée. Nécessite-t-elle des notions informatiques avancées ? Existe-t-il une aide en ligne, un manuel d'utilisation ? Les moyens utilisés pour sécuriser le système (chiffrement des informations stockées, ou comptes multiples d'administration) ont aussi été évalués.

■ GESTION DES VULNÉRABILITÉS

Nous nous sommes intéressés à la classification des vulnérabilités, aux synchronisations possibles avec d'autres bases de données, et à la façon de gérer les correctifs.

COEFFICIENTS DE PONDÉRATION

La note globale a été établie selon les coefficients de pondération suivants : pertinence de l'audit, 3 ; inventaire et découverte, 2,5 ; rapports et alertes, 2 ; facilité d'emploi et sécurité, 1,5 ; et gestion des vulnérabilités, 1.

LA PLATE-FORME DE TEST

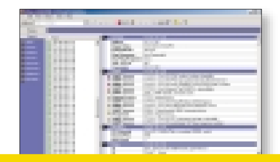
Chaque solution (Retina Network Security Scanner, Internet Scanner, et Nessus avec Lightning Console) a été installée sur un serveur distinct. Le logiciel scanner et la console composant chaque solution ont été déployés sur le même serveur, pour ne piloter qu'un seul scanner à chaque fois. Après leur mise à jour, les logiciels ont été figés afin de les tester en l'état. Rappelons que QualysGuard Intranet Scanner est un service en ligne.



LES PRINCIPALES CARACTÉRISTIQUES

	EEYE DIGITAL SECURITY **Retina Network Security Scanner**	INTERNET SECURITY SYSTEMS **Internet Scanner**	QUALYS **QualysGuard Intranet Scanner**	TENABLE **Nessus et Lightning Console**
Version testée	Retina 4.9.153	7.0 2003 310 (XPU16)	Scanner : 1.14.53-1 ; signature : 1.6.107-3	Nessus 2.0.9 et Lightning Console 2.0.3
Prix (ht)	6 060 € (256 adresses)	11 000 € (250 adresses)	40 000 €/an (250 adresses)	7 996 € (255 adresses)
Possibilité pour la console de piloter plusieurs scanners logiciels	**oui** (avec module logiciel REM)	**oui** (avec module SiteProtector)	Non applicable	**oui**
> Inventaire du réseau				
Fonctionnement du scanner via un routeur IP	**oui**	**oui**	**oui**	**oui**
Possibilité d'importer une liste d'adresses IP issue d'un autre outil	**oui**	**oui**	**non**	**non**
Détection d'un changement de machine (sans changement d'adresse IP)	**non**	**non**	**non**	**non**
Mode découverte	**oui**	**oui**	**oui**	**non**
> Réglages possibles				
Politique de sélection des tests	**oui**	**oui**	**oui**	**oui**
Possibilité de scanner plusieurs machines IP simultanément	**oui**	**oui**	**oui**	**oui**
Possibilité de générer des attaques intrusives	**oui**	**oui**	**non** (prévu en juin 2004)	**oui**
Possibilité de scanner de façon exhaustive et automatique des machines modifiées	**non**	**oui**	**oui**	Non constaté
> Gestion des vulnérabilités				
Tableau de bord de suivi des interventions	**oui** (avec REM)	**non**	**oui**	**oui**
Préconisation de mises à jour	Non communiqué	**oui**	**oui**	**oui**
Génération automatique d'un profil d'audit ciblé sur la vérification des corrections	non	non	non	non
> Types de rapports				
Par type de machine	**oui**	**non**	**oui**	**oui** (via filtre Asset)
Par système d'exploitation	**non**	**non**	**oui**	**oui** (via filtre Asset)
Par niveau de risque	**non**	**oui**	**oui**	**oui**
Format des fichiers de rapport	HTML et XML	HTML, PDF et RTF	HTML, XML, MHT et PDF	PDF et HTML zippé
> Déclenchement d'alertes				
Sur fréquence de vulnérabilité	**non**	**non**	**non**	**non**
Sur vulnérabilité de machines stratégiques	**oui**	**non**	**non**	**oui**
Alertes envoyées	**oui** (par e-mail)	**non**	**non**	**oui** (par e-mail)
> Facilité d'emploi et sécurité				
Suivi en temps réel des audits	**oui**	**oui**	**oui**	**non**
Possibilité de programmer les audits dans le temps	**oui**	**non**	**oui**	**oui**
Chiffrement entre la console et le scanner	Scanner et console sur la même machine	**oui**	**oui**	**oui** (via SSL)
Stockage sécurisé des résultats	**oui**	**non**	**oui**	**non**
Envoi sécurisé des rapports	**non**	**non**	**oui** (par téléchargement)	**oui** (en option)
Gestion de comptes avec droits limités	**oui** (avec REM)	**oui** (avec SiteProtector)	**oui**	**oui**

 LA SYNTHÈSE PRODUIT PAR PRODUIT



EEYE DIGITAL SECURITY
Retina Network Security Scanner

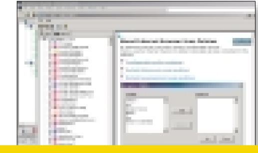
INTERFACE SOIGNÉE ET BONS RAPPORTS

Ce logiciel fonctionne sous Windows 2000 et SQL 2000, qu'il faut préalablement installer. Il convient ensuite de mettre en place tous les modules, et de les interfacer. Il faut alors créer la base de mesure via un script. Retina Network Security Scanner est capable de détecter et d'identifier des systèmes d'exploitation autres que Windows, comme Unix ou Linux, ainsi que des équipements de réseau, routeurs ou commutateurs. Notre laboratoire a testé la version 4.9.153.
Le scanner et la console sont sur le même serveur, ce qui évite de sécuriser les échanges de données entre eux. La licence logicielle est commercialisée pour une classe d'adresses IP. Le scanner fonctionne de pair avec plusieurs autres modules logiciels qui tiennent le rôle d'une console centralisée de visualisation et d'administration sous l'appellation unifiée REM.

 **POINTS FORTS**
- **Qualité de la présentation du rapport**
- **Fonction de découverte**
- **Possibilité de définir une politique d'audit**

 **POINTS FAIBLES**
- **Gestion des correctifs via un module en option**
- **Manque de finesse du classement des vulnérabilités**

Critères	Notes sur 10
Pertinence de l'audit	6,2
Inventaire et découverte	6,3
Rapports et alertes	5,7
Facilité d'emploi et sécurité	6,4
Gestion des vulnérabilités	2,6
Note globale pondérée	**5,8**



INTERNET SECURITY SYSTEMS
Internet Scanner

PERTINENT SURTOUT EN WINDOWS

Le produit d'Internet Security Systems fonctionne sous Windows 2000 ou XP. La version testée par notre laboratoire est la 7.0. Elle repose sur une architecture de type client-serveur incluant scanner, console et base de données (SQL Server 2000 avec MSDE fourni). La console déportée est gratuite, mais il faut penser à installer le scanner pour gérer la communication.
Il est aussi possible d'intégrer un module logiciel gratuit, SiteProtector, qui n'a pas été testé. Celui-ci permet de gérer de façon centralisée plusieurs solutions de l'éditeur, et de bénéficier d'une interface de console plus récente avec des possibilités avancées de *reporting*. La tarification de la licence s'effectue selon le nombre de machines à scanner.

 **POINTS FORTS**
- **Visualisation des résultats du *scan* en temps réel**
- **Rapports bien présentés**
- **Possibilité d'activer des tests intrusifs**

 **POINTS FAIBLES**
- **Résultats stockés dans la base non chiffrés par défaut**
- **Pauvreté des détails du rapport technique d'audit**

Critères	Notes sur 10
Pertinence de l'audit	5,5
Inventaire et découverte	6,2
Rapports et alertes	4,1
Facilité d'emploi et sécurité	6,7
Gestion des vulnérabilités	5,5
Note globale pondérée	**5,6**



pour petits et moyens sites

QUALYS
QualysGuard Intranet Scanner

AUDIT PERTINENT, INVENTAIRE COMPLET

Cette solution repose sur un boîtier installé dans l'entreprise et connecté sur le réseau local à surveiller. Sa commercialisation s'effectue sous la forme d'un service sans acquisition de licence logicielle. Le boîtier est relié en IP à travers internet avec un service distant hébergé et géré par Qualys. Entièrement propriétaire, il repose sur un noyau logiciel Linux Red Hat renforcé, avec un disque dur dont les données sont chiffrées. Il communique exclusivement via le port 443 (utilisé par SSL) vers le service en ligne distant de Qualys.
QualysGuard Intranet Scanner cible la détection de routeurs, de commutateurs, de pare-feu, de serveurs web, NT et Unix, ou d'imprimantes. Sa tarification se décline, outre le prix du boîtier, en fonction du nombre d'adresses scannées, mais pour un nombre illimité de scans.

 **POINTS FORTS**
- **Inventaire très détaillé**
- **Cartographie du réseau**
- **Gestion des interventions, et suivi des correctifs**

 **POINTS FAIBLES**
- **Absence de test intrusif sur la version testée**
- **Absence de mode découverte**

Critères	Notes sur 10
Pertinence de l'audit	6,9
Inventaire et découverte	7,6
Rapports et alertes	8,1
Facilité d'emploi et sécurité	8,7
Gestion des vulnérabilités	8,2
Note globale pondérée	**7,7**



TENABLE
Nessus et Lightning Console

UN BON OUTIL ISSU DE L'OPEN SOURCE

Couplé au logiciel d'administration Lightning Console, qui fonctionne sous Linux Red Hat ou Mac OS X, le logiciel de *scan* Nessus est issu du monde de l'*open source*. Il fonctionne avec Linux et, de préférence, Red Hat. Lightning Console a été installé sur Red Hat 9. Des notions en informatique sont indispensables, même si la documentation est fournie. L'interface utilisateur, bien que graphique, est peu synthétique, et il n'y a pas d'aide en ligne, ni d'assistant logiciel.
Il n'y a pas non plus de mode découverte : le premier *scan* va détecter la configuration de chaque machine du parc, et ajouter cet inventaire dans la base de données Nessus. Notez, enfin, qu'il existe un CD pour installer automatiquement les deux logiciels.

POINTS FORTS
- **Gestion des interventions, et suivi des correctifs**
- **Contrôle centralisé de plusieurs scanners**
- **Envoi automatique de rapports**

 **POINTS FAIBLES**
- **Déploiement peu ergonomique**
- **Manque de suivi en temps réel du déroulement de l'audit**
- **Absence de mode découverte**

Critères	Notes sur 10
Pertinence de l'audit	6,1
Inventaire et découverte	6,8
Rapports et alertes	7,5
Facilité d'emploi et sécurité	6,5
Gestion des vulnérabilités	7,6
Note globale pondérée	**6,8**